ISSN 2303-4521
Original Research

Periodicals of Engineering and Natural Sciences
Vol. 10, No. 1, January 2022, pp.288-294

A novel secure artificial bee colony with advanced encryption standard technique for biomedical signal processing

Brwa Khalil Abdullah Ahmed[1], Rasha Dheyaa Mahdi [2], Tarek Ismail Mohamed[3], Refed Adnan Jaleel[4], Mohanad Ahmed Salih[5], Musaddak Maher Abdul Zahra[6a,b]

[1]Shaqlawa technical college, Erbil polytechnic University, Management Information System, Iraq
[2]Technical Engineering Collage, Northern Technical University (Ntu), Mosul, Iraq
[3]College of Mass Communication, Ajman University, Ajman, U.A.E
[4]Dept. of Information & Communication Engineering, Al-Nahrain University, Iraq
[5]Dept. of Computer Science, Al-Anbar University, Iraq
[6a] Dept. of Computer Tech. Engineering, Al-Mustaqbal University College, Iraq
[6b] Dept. of Electrical Engineering, University of Babylon, Iraq

ABSTRACT

Over the years, the privacy of a biomedical signal processing is protected using the encryption techniques design and meta-heuristic algorithms which are significant domain and it will be more significant shortly. Present biomedical signal processing research contained security because of their critical role in any developing technology that contains applications of cryptography and health deployment. Furthermore, implementing public-key cryptography in biomedical signal processing sequence testing equipment needs a high level of skill. Whatever key is being broken with enough computing capabilities using brute-force attack. As a result, developing a biomedical signal processing cryptography model is critical for improving the connection between existing and emerging technology. Furthermore, public-key cryptography implementation for meta-heuristic-based bio medical signal processing sequence test equipment necessitates a high level of skill. The suggested novel technique can be used to develop a secure algorithm of artificial bee colony, which depend on the advanced encryption standard (AES). AES can be used to reduce the encryption time and to increase the protection capacity for health systems. The novel secure can protect the biomedical signal processing against plain text attacks.

Keywords: AES, ABC, BSP, Encryption, Optimization

Corresponding Author:

Refed Adnan Jaleel
Information and Communication Engineering
Al-Nahrain University
Baghdad, Iraq
E-mail: Iraq_it_2010@yahoo.com

1. Introduction

The science of protecting the information of communications and messages is known as cryptography. The other sub discipline, cryptanalysis, aims to undermine or overcome cryptography's security [1] [2]. Cryptanalysis and cryptography are built on the foundation of mathematics. Cryptography is most usually connected with encryption, which is the process of transforming information and data into a format that is inaccessible to anybody who is not permitted to see it. In the most industrialized countries and areas, the population of middle-aged and elderly individuals predominates, necessitating government intervention to address health-care issues [3] [4]. This leads in a shortage of working adults to care for the growing senior population, potentially causing financial problems while also lengthening the time it takes for a patient to obtain treatment [5] [6]. As a result, newer solutions are needed to improve the level of automation from current systems and to handle the massive amounts of data generated, stored, and sent between them in a safe and efficient manner. [7] [8]. In this paper, the field of AES using ABC for biomedical signal processing is suggested, it encompasses the measurement and digitization of patient monitoring such as the transmission of packets over a wireless network and the delivery of medical data to health-care experts, as well as blood pressure and electrocardiograms (ECGs). The study aims to build a novel secure technique incorporating biomedical signal, the AES algorithm which implemented and integrated with the biological environment, and artificial bee colony. By generating primary key and rule keys, this technique can protect biological signals sent through optimal healthcare systems platforms from plain text attacks. The study makes several achievements, including (I) the algorithm of multilayer encryption that integrates the algorithm of AES, and biomedical signal processing, (ii) an encryption technique which is reliable for the systems of artificial bee colony-based healthcare, (iii) a technique of encryption that reduces the message length of ECG and thus reduces complicated mathematical operations, (iv) the technique of encryption that enhances the encryption power and offers better security and much more complex to the multilayer ABC and AES.

2. Material and methods

2.1. Biomedical Signal Processing

Bio-medical signal processing is primarily concerned with the novel applications of the methods of processing signals to biomedical signals via numerous innovative collaborations of biomedical knowledge with the method [9]. It is indeed a fast - growing field with numerous applications [10]. These vary from the development of artificial limbs and assistive devices for the disabled to the creation of advanced systems of medical monitoring which can perform noninvasively to provide real-time views of human body workings [11]. There are a different kinds of common used medical systems. Ultrasound, plythesmography, and electrocardiography are all utilized for a variety of reasons. Figure 1 depicts the stages of biosignal processing [12].

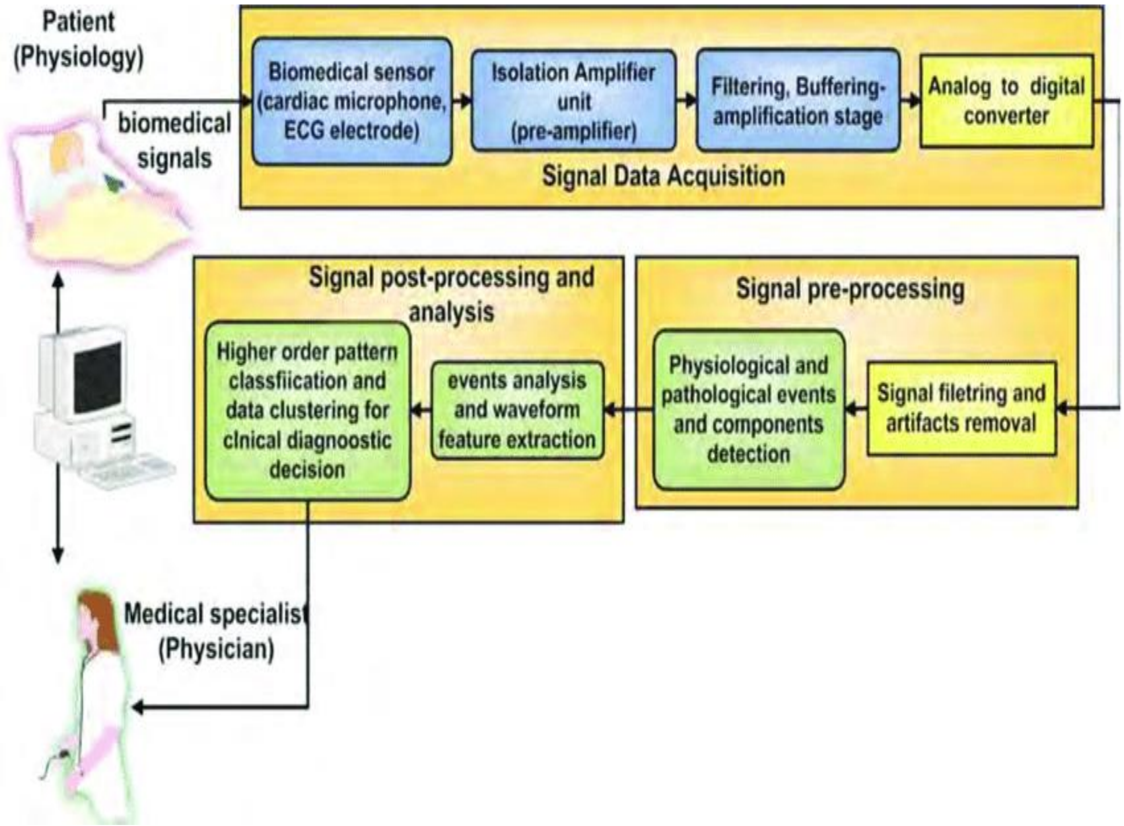
Patient
(Physiology)
biomedical signals
Biomedical sensor (cardiac microphone, ECG electrode)
Isolation Amplifier unit (pre-amplifier)
Filtering, Buffering-amplification stage
Analog to digital converter
Signal Data Acquisition
Signal post-processing and analysis
Higher order pattern classfiication and data clustering for clnical diagnoostic decision
events analysis and waveform feature extraction
Signal pre-processing
Physiological and pathological events and components detection
Signal filetring and artifacts removal
Medical specialis
(Physician)

Figure 1. Block diagram of the general biomedical signal processing

2.2. Artificial bee colony

In 2005, Karaboga proposed the algorithm of Artificial Bee Colony (ABC) for enhancing numeric problems. The algorithm's authors, along with some researchers, provided many such developments [13] [14]. The ABC algorithm is based on honey bee swarms that represent bee swarms' intelligent foraging actions. It is a stochastic optimization algorithm that is population based, very simple, and robust. A honey bees' swarm could complete tasks successfully by social cooperation [15]. Three types of bees in the ABC algorithm: scout bees, onlooker bees, and employed bees. The food searching around the source of food throughout their memory is in the employed bees , while onlooker bees exchange information about that food sources [16]. Onlooker bees goal is to select better food sources among employed bees sources discovered [17]. The food source with higher quality (fitness) will be chosen over the one with lower quality by onlooker bees [18]. According to the ABC algorithm, the employed bees is the first half of the swarm, while the second half is made up of onlooker bees. the derived from a small number of employed bees is the scout bees that are let down the sources of food in discovery of better ones. This is clear from the ABC algorithm's general flow chart (depict in Figure 2) [17].

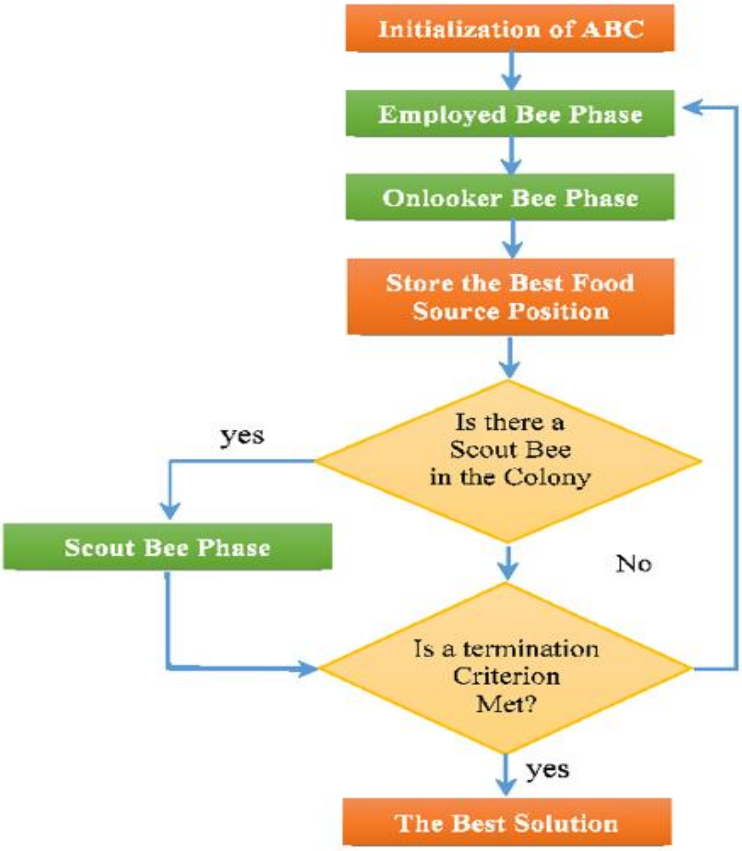
Initialization of ABC
Employed Bee Phase
Onlooker Bee Phase
Store the Best Food Source Position
Is there a Scout Bee in the Colony
yes
Scout Bee Phase
No
Is a termination Criterion Met?
yes
The Best Solution

Figure 2. Flowchart of ABC algorithm

2.3. Advanced encryption standard

AES was a top contender in the NIST competing and was named the most strong encryption algorithm in October 2000 [19] [20]. It is also recognized as Rijndael and has a variable key length of 256 bits, 192 bits, r o128 bits with 128 bits fixed-block size[21] [22]. AES is an algorithm which is symmetric with a private key that is used for encryption/decryption processes. Each round of AES encryption-decryption processes consists of four basic stages. ShiftRows is the permutation stage, and the remaining are three substitution stages that are byte Substitute, MixColumn, and AddRundKey [23] [24]. Figure 3 depicts the Advanced Encryption Standard algorithm's encryption and decryption procedures [25].

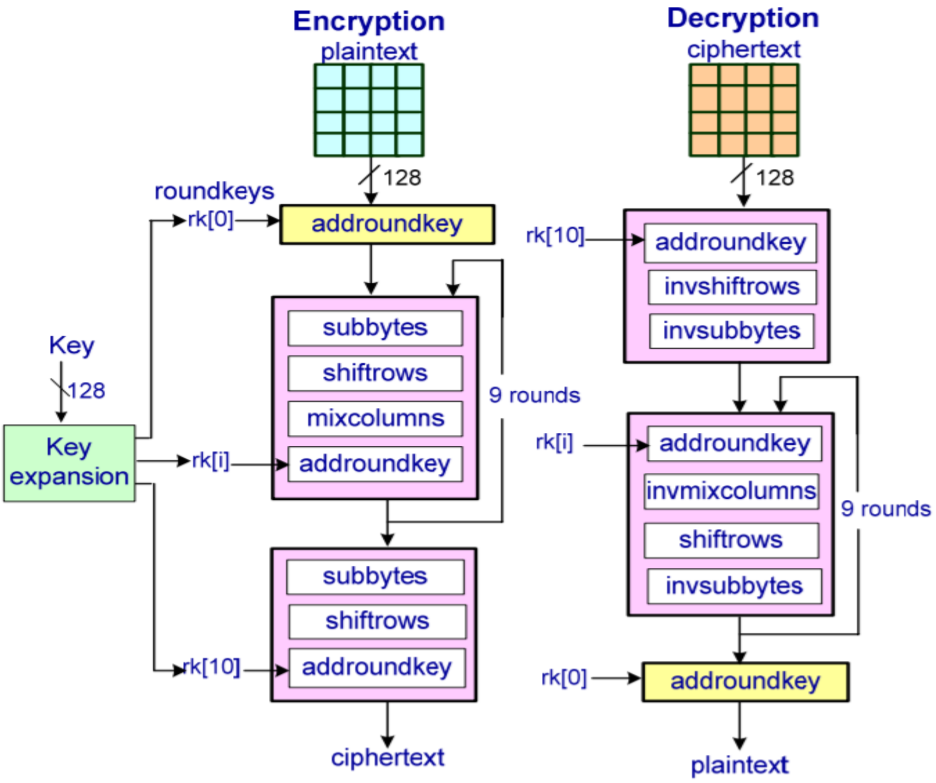

Figure 3. AES algorithm for encryption and decryption

3. Results and discussion

Researchers in the field of biomedical research have access to an ever-expanding database of digital recordings of biological signals and related data. Encryption quality are all included in the experimental analysis. This is the most important test for demonstrating the given algorithm's good security. The encryption and decryption throughput of algorithms without and with ABC can be calculated using encryption and decryption time. The algorithm's taken time for encrypt/decrypt inputted ECG signals is one of the performance parameters. A total of 20 experiments were conducted to ensure that no one participant's results were influenced by their own bias. Table 1 offers the decryption and encryption execution time with ABC and without ABC. Figures of the ECG shown in Figure 4 and Figure 5 for original signal and cipher signal.

Table 1. Time of encryption and decryption

Number of rounds	AES	AES	AES with ABC	AES with ABC
	Encryption Time	Decryption Time	Encryption Time	Decryption Time
1	30.44	45.87	20.99	32.84
2	27.21	43.22	19.22	30.29
3	27.22	44.10	19.21	31.64
4	26.13	42.76	18.22	29.21
5	26.27	40.13	17.99	27.54
6	26.55	40.14	17.87	27.23
7	25.11	39.24	16.98	26.55
8	29.29	45.88	20.25	32.76
9	24.87	38.41	17.23	25.22
10	31.56	47.24	22.78	39.35
11	22.12	34.11	12.48	29.44
12	22.58	34.78	12.22	29.82
13	23.69	35.99	14.77	30.25
14	22.11	35.89	12.24	30.12

Number of rounds	AES	AES	AES with ABC	AES with ABC
	Encryption Time	Decryption Time	Encryption Time	Decryption Time
15	21.87	37.12	14.89	32.89
16	20.11	36.67	11.74	30.99
17	19.99	34.97	9.21	28.49
18	18.33	33.54	8.98	27.83
19	17.23	32.15	7.93	29.11
20	12.44	27.81	4.88	24.87

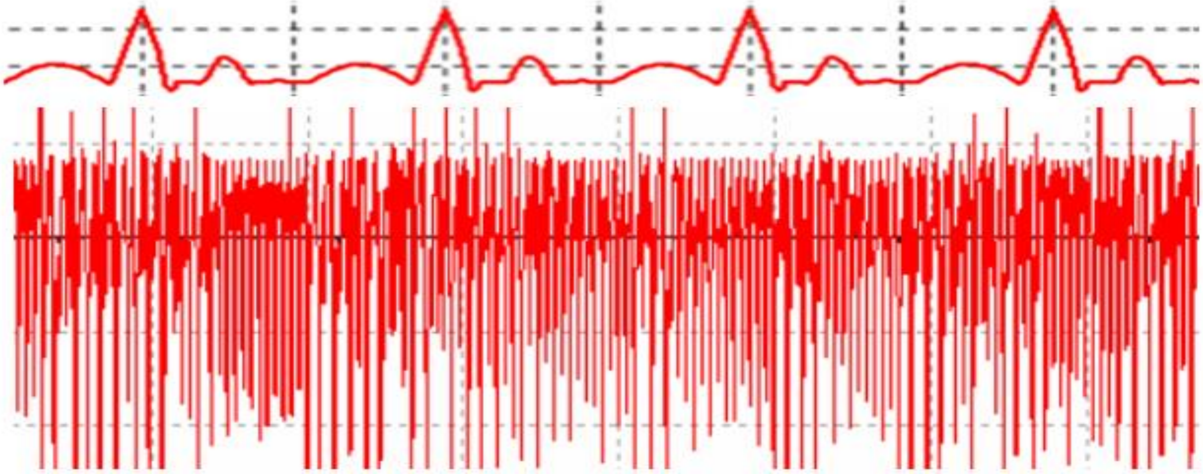

Figure 4. Original and cipher ECG without ABC

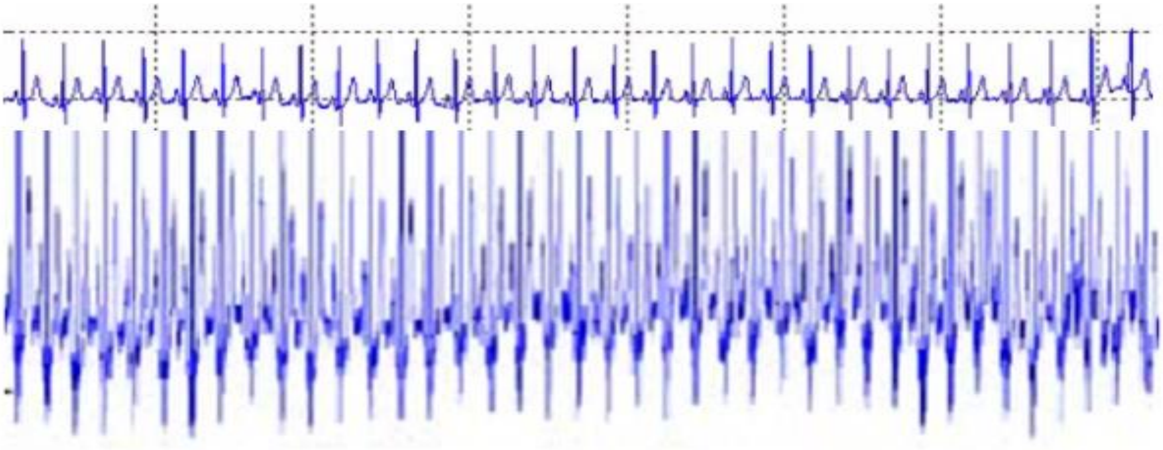

Figure 5. Original and cipher ECG with ABC

4. Conclusions

This study presents a novel secure technique incorporating ABC and AES algorithm for biomedical signal processing, which reduces the message length of biomedical signal and the complicated mathematical operations which use much more resources and took a more processing time. A novel technique employs keys provided by AES standards that enhances the power of encryption while also providing increased complexity and security. The needed breaking time of decryption has been significantly increased. The concepts of AES and ABC computing combination improves the encryption and decryption procedures. The results indicate that combining ABC and AES outperforms the original algorithm of AES. Experiment results show that a novel technique gives a high-level of integrity, security, robustness, and efficiency. In fact, the field of joint encryption is ripe for investigation.

References

[1] H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, *arXiv preprint arXiv*, 003.06557, 2020.

[2] M. Nikooghadam and H. Amintoosi, “A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol”, *Security and Privacy*, vol. *3*, no. 1, e92. 2020.

[3] C. Kessler and M. Philips, “Cryptography, Passwords, Privacy, and the Fifth Amendment”, *Journal of Digital Forensics, Security and Law*, vol. 15, no. 2, pp. 2, 2020.

[4] S. Rajvir et al., “Image encryption using modified elliptic curve cryptography and Hill cipher”, *Smart Intelligent Computing and Applications* (pp. 675-683). Springer, Singapore. 2020.

[5] P. Pain, et al., “Quantum Random Number Generators for Cryptography: Design and Evaluation”, *Computational Advancement in Communication, Circuits and Systems* (pp. 315-322). Springer, Singapore, 2020.

[6] V. Sánchez, et al., “Survey on physical layer security for 5G wireless networks”, *Annals of Telecommunications*, vol. 76, no. 3, pp. 155-174, 2021.

[7] M. Fama, S. Lucarelli, and R. Orzi, “Rethinking Money, Rebuilding Communities: A Multidimensional Analysis of Crypto and Complementary Currencies”. *Partecipazione e conflitto*, vol. 13, no. 1, pp. 337-359, 2020.

[8] J. Eterovic, M. Cipriano, E. Garcia, and L.Torres, “Lightweight Cryptography in IIoT the Internet of Things in the Industrial Field” *Argentine Congress of Computer Science* (pp. 335-353). Springer, Cham. 2019.

[9] N. Jain, B.Mishra and P. Wilson, “A Low gate count reconfigurable architecture for biomedical signal processing applications”. *SN Applied Sciences*, vol. *3*, no. 4, pp. 1-19, 2021.

[10] A.Colominas, G. Schlotthauer, and E. Torres, “Improved complete ensemble EMD: A suitable tool for biomedical signal processing”. Biomedical Signal Processing and Control, vol. 14, pp. 19-29, 2014.

[11] J. Rafiee, et al., “Wavelet basis functions in biomedical signal processing”. *Expert systems with Applications*, vol. 38, no. 5, 6190-6201, 2011

[12] K. Abbas and R. Bassam, “Phonocardiography signal processing”. *Synthesis Lectures on Biomedical Engineering*, vol. 4, no. 1, pp. 1-194, 2009.

[13] H. Wang, et al., “Improving artificial bee colony algorithm using a new neighborhood selection mechanism”. *Information Sciences*, vol. 527, pp. 227-240, 2020.

[14] Y. Li, et al, “An improved artificial bee colony algorithm for distributed heterogeneous hybrid flowshop scheduling problem with sequence-dependent setup times”. *Computers & Industrial Engineering*, vol. 147, 106638. 2020.

[15] N. Rahnema and S. Gharehchopogh, “An improved artificial bee colony algorithm based on whale optimization algorithm for data clustering”. *Multimedia Tools and Applications*, vol. 79, no.43, pp. 32169-32194, 2020.

[16] S. Öztürk, R. Ahmad and N. Akhtar, “Variants of Artificial Bee Colony algorithm and its applications in medical image processing”. *Applied Soft Computing*, 106799. 2020.

[17] Q. Li and Q. Han, “A hybrid multi-objective artificial bee colony algorithm for flexible task scheduling problems in cloud computing system”. *Cluster Computing*, vol. 23, 4, pp. 2483-2499, 2020.

[18] J. Sengathir , “A novel cluster head selection using Hybrid Artificial Bee Colony and Firefly Algorithm for network lifetime and stability in WSNs,” CONNECTION SCIENCE2021, AHEAD-OF-PRINT, 1-22, https://doi.org/10.1080/09540091.2021.2004997

[19] H. Ghanen and A. Jantan, “Using hybrid artificial bee colony algorithm and particle swarm optimization for training feed-forward neural networks”. *Journal of theoretical & applied information technology*, vol. 67, no. 3, 2014.

[20] E. Hameed, M. Ibrahim, and N. Abd Manap, “Compression and encryption for ECG biomedical signal in healthcare system,” T*elkomnika,* vol. 17, no.6, pp. 2826-2833, 2019.

[21] J. Madhloom, K. Abd Ghani, and R. Baharon, “ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing. *Intelligent automation and soft computing*, vol. 28, no. 2, pp. 493-512, 2021.

[22] Z. Rahaman, et al., “A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix”, *arXiv preprint arXiv: 2005.00157*.2020.

[23] Z. Kasiran, S. Abdullah, and M. Nor, “An advance encryption standard cryptosystem in iot transaction,”*Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, pp. 1548-1554, 2020.

[24] I. Salih, A. Alabaich, and Y. Tuama, “Enhancing advance encryption standard security based on dual dynamic XOR table and mixcolumns transformation,”*Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 3, pp. 1574-1581, 2020.

[25] A. Nadjia and A. Mohamed, “Aes ip for hybrid cryptosystem rsa-aes,”*2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15)*, pp. 1-6, *IEEE*, 2015.